This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

BLACK BORDERS

IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

FADED TEXT OR DRAWING

BLURRED OR ILLEGIBLE TEXT OR DRAWING

SKEWED/SLANTED IMAGES

COLOR OR BLACK AND WHITE PHOTOGRAPHS

GRAY SCALE DOCUMENTS

LINES OR MARKS ON ORIGINAL DOCUMENT

REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

IMAGES ARE BEST AVAILABLE COPY.

OTHER:

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

0 = Full sian

	\mathcal{C}			
L Number	Hits	Search Text	DB	Time stamp
- Number	5	ingrian.as.	USPAT;	2004/09/30
	\	111911 tall. ab.	US-PGPUB;	06:57
	1		EPO; JPO;	
			IBM TDB	
	1	("6081900").PN.	USPAT;	2004/09/27
_	1	("6081900").PN.	US-PGPUB;	09:44
			EPO; JPO;	05.44
	1	`	i i	
	//	1	IBM_TDB	2004/00/27
_	/15 /	/ingrian.as.	USPAT;	2004/09/27
			US-PGPUB;	13:46
			EPO; JPO;	
	j		DERWENT;]
			IBM_TDB	
_	0	(@ad<20000612 and (rsa same (efficien\$3))	USPAT;	2004/09/27
	1 1	and (chinese)) and (hensle hensel)	US-PGPUB;	13:47
			EPO; JPO;	
			DERWENT;	!
	ABS //	· ·	IBM TDB	•
_	+./ 19	<code>dead<20000612 and (rsa same (efficien\$3))</code>	USPAT;	2004/09/30
	tuly 19	and (chinese)	US-PGPUB;	09:22
	P /	and (Chinese)	EPO; JPO;	
			DERWENT;	
			IBM TDB	
) (W160W 11 145m)	USPAT;	2004/09/28
	386	rsa and ("160" adj bits)	USPAT; US-PGPUB;	10:16
			1	10.10
		,	EPO; JPO;	
		. "	IBM_TDB	2004/00/20
_	. 27	rivest.in.	USPAT;	2004/09/28
			US-PGPUB;	13:41
		, ,	EPO; JPO;	
			IBM_TDB	
_	1	"20020087884"	USPAT;	2004/10/01
	_	20020001001	US-PGPUB;	08:07
	Ì		EPO; JPO;	
			IBM TDB	
		/#4 242 117#\ DN	USPAT;	2004/09/29
	1	("4,242,117").PN.	US-PGPUB;	07:29
			EPO; JPO;	1 0 1 1 2 2
			IBM TDB	
		1 /	USPAT;	2004/09/29
- '	/ 8	(boneh.in. shacham.in. beri.in.) and		07:40
	/ /	(rsa)	US-PGPUB;	07:40
			EPO; JPO;	1
	· .		DERWENT;	
			IBM_TDB	
_	ABS 7	minimiz\$3 with (disparity difference)	USPAT;	2004/09/29
	1は1	with exponents)	US-PGPUB;	07:41
	will	•	EPO; JPO;	
	'		DERWENT;	
			IBM TDB	
	216	rsa and ((reduc\$3 minimiz\$5) with (prime	USPĀT;	2004/09/29
_	710	p q)) and (m n modulus pq)	US-PGPUB;	07:43
		p q// and (m n modulus pq/	EPO; JPO;	
			DERWENT;	
			IBM TDB	
		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		2004/09/29
_	100	rsa and ((reduc\$3 minimiz\$5) with (prime	USPAT;	· ·
	1	p q)) and ((m n modulus pq) with	US-PGPUB;	07:43
	1	constan\$5)	EPO; JPO;	
	1		DERWENT;	
	1		IBM_TDB	
_	45	(rsa and ((reduc\$3 minimiz\$5) with (prime	USPAT;	2004/09/29
	1	p q)) and ((m n modulus pq) with	US-PGPUB;	08:02
	1	constan\$5)) and @ad<20010612	EPO; JPO;	
		Composition / and care to be a control of the	DERWENT;	
			IBM TDB	
		((rsa and ((reduc\$3 minimiz\$5) with	USPAT;	2004/09/29
_	43	((Isa and ((Ieddc3) minimiz3)) with	US-PGPUB;	08:13
		(prime p q)) and ((m n modulus pq) with		55.15
	Ì	constan\$5)) and @ad<20010612) and ("1/3"	EPO; JPO;	
		third three)	DERWENT; IBM TDB	Ì

-			((rsa and ((reduc\$3 minimiz\$5) with (prime p q)) and ((m n modulus pq) with	USPAT; US-PGPUB;	2004/09/29 08:02
			constan\$5)) and @ad<20010612) and ("1/3"	EPO; JPO; DERWENT;	
			third)	IBM_TDB	
-	ABO /	23	(((rsa and ((reduc\$3 minimiz\$5) with (prime p q)) and ((m n modulus pq) with	USPAT; US-PGPUB;	2004/09/29 08:14
E	vivia .	/ I	constan\$5)) and @ad<20010612) and ("1/3"	EPO; JPO;	
		ا ا	third three)) not silverbrook.in.	DERWENT; IBM TDB	
_		$\binom{7}{6}$	((((rsa and ((reduc\$3 minimiz\$5) with	USPAT;	2004/09/29
	1 (X	(prime p q)) and ((m n modulus pq) with constan\$5)) and @ad<20010612) and ("1/3"	US-PGPUB; EPO; JPO;	08:14
] -	third three)) not silverbrook.in.) not	DERWENT;	
			(((rsa and ((reduc\$3 minimiz\$5) with (prime p q)) and ((m n modulus pq) with	IBM_TDB	1
			constan\$5)) and @ad<20010612) and ("1/3"		,
	1		third)) compaq.as. and (multi adj prime)	USPAT;	2004/09/29
-		0	compaq.as. and (multi ad) prime,	US-PGPUB;	09:40
	3			EPO; JPO; IBM TDB	
_	7 ith	18	compaq.as. and rsa	USPAT;	2004/09/29
	Scaring	Å	-	US-PGPUB; EPO; JPO;	09:40
	Son /	\sim	·	IBM_TDB	2024/02/20
-		0	compaq.as. and rsa and ssl	USPAT; US-PGPUB;	2004/09/29 09:46
				EPO; JPO;	
	ļ	1	("5848159").PN.	<pre>IBM_TDB USPAT;</pre>	2004/09/29
_		1	(5040139). FW.	US-PGPUB;	10:29
				EPO; JPO; IBM TDB	
_		2	("4405829").PN.	USPAT;	2004/09/29
		Ì		US-PGPUB; EPO; JPO;	10.30
			lander	IBM_TDB USPAT;	2004/09/29
-		1	(("4405829").PN.) and (size bit lenght)	US-PGPUB;	10:30
				EPO; JPO; IBM TDB	
_		799	rsa and ((private adj key) same random)	USPAT;	2004/09/29
		,,,,	(12	US-PGPUB; EPO; JPO;	10:38
		!		IBM_TDB	
-		494	rsa and ((private adj key) with random)	USPAT; US-PGPUB;	2004/09/29 10:38
		ļ		EPO; JPO;	
1		E 2 1	rsa and ((private adj key) with random\$2)	IBM_TDB USPAT;	2004/09/29
-		221	isa and ((private ad) key, with randomyz)	US-PGPUB;	10:38
	ASS)	EPO; JPO; IBM TDB	
_	17.1/	35	@ad<20000612 and rsa same ((private adj	USPAT;	2004/09/29 10:49
	will		key) with random\$2)	US-PGPUB; EPO; JPO;	10.49
			,	IBM_TDB	2004/09/29
-		101	<pre>@ad<20000612 and rsa same ((private adj key) with (length bit))</pre>	USPAT; US-PGPUB;	10:50
	-1	10		EPO; JPO; IBM TDB	
_	ABS	4 1	ead<20000612 and rsa same ((private adj	USPĀT;	2004/09/29
	world	/3	key) with (length bit size)) and ("public key" with (length bit size))	US-PGPUB; EPO; JPO;	10:50
1	' \		D .	IBM TDB	2004/00/00
-	/	/ 5	(hensle hensel) adj lift\$3) and rsa	USPAT; US-PGPUB;	2004/09/29 11:15
	'(EPO; JPO;	
	1			IBM TDB	

	T 15 I	hensel adj lift\$3	USPAT;	2004/09/29
_	12	Henser and rereas	US-PGPUB;	15:44
	1		EPO; JPO;	,
			DERWENT;	
	1	·	IBM TDB	
	_	(UCERCOAU) DN	USPAT;	2004/09/30
_	1	("6735694").PN.	US-PGPUB;	07:00
			EPO; JPO;	07.00
				ļ
			IBM_TDB USPAT;	2004/09/30
_	1	("5875296").PN.		07:46
			US-PGPUB;	07:46
			EPO; JPO;	
			IBM_TDB	
_	. 1	("6085030").PN.	USPAT;	2004/09/30
			US-PGPUB;	09:15
			EPO; JPO;	
	ABS 5	()	IBM_TDB	
_	5	session adj integrity adj key	USPAT;	2004/09/30
}	10/21/	V	US-PGPUB;	09:15
	1) may	·	EPO; JPO;	
	[· ·	IBM TDB	
	919	rsa and (bits near (long length))	USPĀT;	2004/09/30
_	919	The did (blob field (tong tong tol)	US-PGPUB;	09:48
			EPO; JPO;	
[IBM TDB	1
		rsa and (bits near (long length)) and	USPAT;	2004/09/30
-	67	(chinese)	US-PGPUB;	09:49
	}	(Chinese)	EPO; JPO;	
			IBM TDB	
		1 (1) and longth \ and	USPAT;	2004/09/30
-	45	rsa and (bits near (long length)) and	US-PGPUB;	09:49
	1	(chinese) and exponent	EPO; JPO;	1 33.43
	1 , ~		IBM TDB	
	hast /	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	USPAT;	2004/09/30
	1 / 22	rsa and (bits near (long length\$2)) and		09:59
/	my /	(chinese) and (exponents roots)	US-PGPUB;	V2:33
	1		EPO; JPO;	l
		,	IBM_TDB	2004/00/20
-	61	rsa and (bits same (exponent\$3 root\$3))	USPAT;	2004/09/30
		and (chinese)	US-PGPUB;	10:00
}			EPO; JPO;	
	1 , 2		IBM_TDB	
l_	DBS /5	rsa and (bits same (exponent\$3 root\$3))	USPAT;	2004/09/30
	1 / °	same (chinese)	US-PGPUB;	10:00
	1-8° .	1 3 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	EPO; JPO;	
	pull		IBM TDB	-

09877655 Michael J. Simitoski Michael.Simitoski@uspto.gov (703) 305-8191

Google

rsa crt "160 bits" chinese remainder "exists a unique element" pair rsa mod(p-1) mod(q-1) crt rsa addition subtraction multiplication division modulo arithmetic rsa (CRT OR chinese) (hensle OR hensel) (lifting) ("1/3" OR third or 3) multi-prime rsa rsa ("chinese remainder" OR CRT) (hensle OR hensel) (efficient OR efficiency) efficient rsa decryption (CRT OR chinese) "Fast Implementation of RSA Cryptography" "techniques for implementing the rsa public" pkcs 8 (chinese OR crt) rsa (third OR "1/3") pkcs 8 (chinese OR crt) rsa (third OR "1/3") multi-prime RSA "chinese remainder" public private rebalanced rsa "Cryptanalysis of Short RSA Secret Exponents" "chinese remainder theorem" ("hensel lifting" OR "hensle lifting") rsa exponent takagi rsa rsa "public key" "private key" bit length bits public key and private key same length

ACM

+author:takagi +rsa +rsa +hensel +rsa "chinese remainder" crt

IEEE

(takagi <in> au) <and> rsa rsa <and> hensel rsa <and> ("chinese remainder" <or> crt)

Other

Search tool webcrawler (with date restriction)

<u>Search Terms</u> RSA "chinese remainder" public private

Applications/Patents from Inventor Search 60/211,023

60/511,031 60/223,171

60/259,786

09/877,302

09/901,350

60/307,672